REMARKS

The application was filed on 19 April 2001 with sixteen claims. The Examiner examined the application and on 21 October 2004 issued a first Action. In the Examiner's Action, the Examiner rejected claims 1-7 and 10-16 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,405, 364 B1 entitled BUILDING TECHNIQUES IN A DEVELOPMENT ARCHITECTURE FRAMEWORK to Bowman-Amuah (Bowman-Amuah '364). The Examiner also rejected claims 8-9 under 35 U.S.C. §103(a) as being unpatentable over Bowman-Amuah '364 in view of U.S. Patent No. 5,519,778 entitled METHOD FOR ENABLING USERS OF A CRYPTOSYSTEM TO GENERATE AND USE A PRIVATE PAIR KEY FOR ENCIPHERING COMMUNICATIONS BETWEEN THE USERS to Leighton et al. (Leighton '778). Applicants responded and amended the specification and claims. The Examiner then finally rejected claims 1-7 and 10-16 under 35 U.S.C. §103(a) as being unpatentable over Bowman-Amuah '364 in view of U.S. Patent No. 4,672,572 entitled PROTECTOR SYSTEM FOR COMPUTER ACCESS AND USE to Alsberg (Alsberg '572); and finally rejected claims 8 and 9 under 35 U.S.C. §103(a) over Bowman-Amuah '364, Alsberg '572, and Leighton '778. Applicants responded in an attempt to put the claims in condition for allowance and/or better condition for appeal. The Examiner did not enter the amendments. Applicants, believing that patentable subject matter persists, filed a Request for Continued Examination.

The Examiner then entered the amendments and rejected claims 1-7 and 10-16 under 35 U.S.C. §103(a) over Bowman-Amuah '364, Alsberg '572 and U.S. Patent No. 6,671,809B1 entitled SOFTWARE-DEFINED COMMUNICATIONS SYSTEM EXECUTION CONTROL to Perona et al. (Perona '809). The Examiner further maintains the same rejection of claims 8-9 under 35 U.S.C. §103(a) over Bowman-Amuah '364, Alsberg '572, and Leighton '778.

Applicants respond by amending the claims. In amending the claims, Applicants have not added new matter. Support in the original filed specification for the invention relating to designing security in an information technology system is given on page 3, line 4. Claims 1-16 are pending.

The Rejection Under 35 U.S.C. §103(a) over Bowman-Amuah '364, Alsberg '572, and Perona '809

The Examiner rejected claims 1-7 and 10-16 under 35 U.S.C. §103(a) as being unpatentable over Bowman-Amuah '364, Alsberg '572, and Perona '809. The Examiner asserts that Bowman-Amuah '364 discloses a system and method for building systems in a development architecture framework wherein security is integrated into the solution. The Examiner admits that Bowman-Amuah '364 does not disclose a security subsystem that includes an audit subsystem, an integrity subsystem, and an information flow control subsystem. The Examiner then relies on Alsberg '572 to provide a protector device for enhancing security including the audit subsystem, integrity subsystem, and information flow control subsystem. Thus, the Examiner reasons that one of skill in the art would be inclined to combine Bowman-Amuah '364 with Alsberg '572 because auditing potentially sensitive material, integrity subsystems, and controlling the information flow would increase the security of the system. The Examiner further admits that Bowman-Amuah '364 does not disclose using a baseline of a security model comprising the security subsystems but asserts that Perona '809 discloses a system that performs rule checks in a two-way manner, restrictions such as licensing and source restrictions may be placed not only on system modules, but also on the applications using the security to be achieved. The Examiner reasons that the modules of Perona '809 include security properties in terms of a plurality of interconnected and interdependent security subsystems, and that one of skill in the art would be motivated to combine the two or three references.

In response, Applicants have amended the claims but still traverse the rejection. Bowman-Amuah '346 teaches an integrated development framework for the creation of software that has security management. The most detail that Bowman-Amuah '364 provides for security management is presented at column 49, line 65 through column 51, line 13. The security management system of Bowman-Amuah '364 deals mainly with preventing unauthorized access to the system, e.g., *intrusion detection, network assessment, platform security to minimize the opportunities for intruders ..., web-based access control, fraud services, mobile code security, e-mail, encryption, public key* *infrastructure, authentication system, and firewall.* Bowman-Amuah '364 briefly mentions the need for security audits for the development architecture framework at column 18, lines 60-63, but merely states that audits can be done by an external body specializing in security in the form of interviews, architecture and code reviews, and automated tool assessment. In other words, Bowman-Amuah '364 considers security to be a separate but equal piece of the integrated development environmental architecture. *See* Figures 2 and 2a. Bowman-Amuah '364 does not start with security subsystems determining the components of the system as Applicants claim; rather Bowman-Amuah '364 starts with designing a development architecture and then tosses security management into the architecture as just another piece of the pie - just like configuration management, release management, quality management, program and project management, problem management, environment management and information management.

Alsberg '572 describes a protector device, also called security server, to be attached to a network of computers and terminals. The security server is intended to be installed after the network has been designed, *that is*, the security server is an afterthought and is "independent from the host computer and terminals but connected to the computers and terminals ...." Alsberg '572 at column 4, lines 1-3.

Applicants continue to traverse the Examiner's alleged combination of Alsberg '572 and Bowman-Amuah '364 because it cannot sustain a prima facie case of obviousness. Alsberg '572 teaches against the desirability of designing security into an already existing architecture, which is the purpose of Bowman-Amuah '364. Alsberg '572 states:

> One technique of preventing undesirable access is to design software that is demonstrably secure. That is, to design software that can be convincingly demonstrated to prevent access by a user to certain unauthorized levels of information and to allow access to certain authorized levels of information. [Applicants comment that the purpose of Bowman-Amuah '364 is to design such software.] *The problem with this technique is that such software typically requires precise design of system functions and structures so that the resulting software is secure against state-of-the-art threats and can be demonstrated to be secure using state-of-the-art technology such as formal verification/proof technology.* In order to add such security to existing software, the architecture of the existing software would have to be significantly

> redesigned. The resemblance of the resulting secure software designed from the preexisting software would be very slight and *would typically destroy compatibility between uses of the existing software and the software which has been made secure*. Alsberg '572 at column 1, lines 17-35. (Emphasis added).

Applicants contend that despite the security server of Alsberg '572 having a command-filter module which generates an audit-capture command only when potentially sensitive information is transmitted, an administrator monitor that has a data base editor, an audit-trail analysis module, a status module, and a system-control module, and a user authentication module that monitors all input from and output to the user terminal; Alsberg '572 teaches away from these security functions being incorporated into the design of an integrated development environment architecture such as one of Bowman-Amuah '364 because of the difficult to design ever-changing software and the on-going difficulties and threats with compatibility.

Perona '809 describes two-way rule checks for a software-defined communications system to enhance security and integrity. Perona '809 is applicable to an open architecture software communication system such as between a computer, a satellite, a cell phone, and any other hardware and software component that will be added. Perona '809 provides rule checks between the platform, i.e., the hardware and operating system, the stored applications, and a plurality of stored modules. Each module is a separate library of software used by the application to execute a specific function to implement the application, e.g., a module may perform data encryption, a different module may perform signal processing, or protocol processing, or network communications planning, or signal modulation, and so on. Every time a new platform or a new application or a new module is added to the open architecture software communications system, the two-way rule checks take place to make sure the software is compatible and licensed with the platform which is compatible and licensed with the modules which is licensed and compatible with the software.

Applicants traverse the rejection under 35 U.S.C. §103(a) based on the alleged combination of Bowman-Amuah '364, Alsberg '572 and Perona '809. Perona '809 teaches away from its combination with Bowman-Amuah '364 because Perona '809 is intended to be used in an open system, i.e., after the communications system has been designed and is in use. Perona '809 provides the two-way rule checks only after new components are added to an existing system; Perona '809 does not teach or suggest that any security management be built into the framework designing the system, and does not rely on security subsystems to determine the properties and functions of the rest of the components of the system, as Applicants claim.

Security management is but one aspect of many of Bowman-Amuah '364 and these other aspects may determine the architecture of the system. Bowman-Amuah '364 further admits that the audit security subsystem or function is independent from the security management system, not an integral, interrelated and interconnected subsystem of security, as Applicants have claimed. Alsberg '572 teaches that a security server should be independent from the information handling system, i.e., the host computer and terminals, in order to avoid "precise design of system functions and structures [taught by Bowman-Amuah '364] so that the resulting software is secure." Perona '809 teaches two-way licensing and compatibility checks that occur only when a new component is added to the system. So, with respect to the Examiner, how can these references possibly be combined? Bowman-Amuah '364 states that the audit function is independent, Alsberg '572 states that the audit function is independent; and Perona '809 states that rules-checking doesn't occur until after a new component has been added to the system. They cannot be combined to yield Applicants' claimed interdependence and interconnectedness among the security subsystems, and then using these security subsystem to define the functions and properties of components of the system.

In view of the amendments and remarks above, Applicants respectfully request the Examiner to withdraw the rejection of claims 1–7 and 10-16 under 35 U.S.C. §103(a) over Bowman-Amuah '364, Alsberg '572, and Perona '809.

The Rejection of claims 8-9 Under 35 U.S.C. §103(a) over Bowman-Amuah '364, Alsberg '572 in view of Leighton '778

The Examiner repeated her rejection of claims 8-9 under 35 U.S.C. §103(a) under a combination of Bowman-Amuah '364 and Alsberg '572 in view of Leighton '778. The Examiner applies Bowman-Amuah '364 and Alsberg '572 as above and then applies

Leighton '778 as a reference to rank the security levels and threats to the system. Applicants repeat their traversal. Applicants reiterate that Bowman-Amuah '364 teaches an integrated development architecture relying on many aspects, other than security, to create the architecture. Bowman-Amuah '364 does not used the interconnectedness and interdependence of at least three security subsystems to define the functions and the properties of the entire system. Alsberg '572 teaches against using the precise detail to design security, such as claimed by Applicants, into a host computer and its terminals because of changing technology; therefore, Alsberg '572 teaches that security functions are best handled by an external security server. Leighton '778 applies a ranking system to users of a cryptosystem wherein communications are ciphered between ranked users of the system, i.e., one user may have a higher security clearance/level than another user. Leighton '778 ranks only those users for secret-key exchange wherein first, users can directly talk to one another and second the conversation between two users always takes place at the highest common level of security, see column 6, lines 44-47. Leighton '778 does not suggest applying a ranking of security threats to the subsystems of a software development system or to an overall information handling system, as claimed by Applicants. Threats to management of audits, integrity, and information flow control are not mentioned by Leighton '778. Thus, with the Examiner's observation that Bowman-Amuah '364 does not rank security threats combined with the fact that Leighton '778 ranks only the security level of users on a cryptographic system, Applicants respectfully request the Examiner to reconsider the rejection of claims 8 and 9 under 35 U.S.C. §103(a) and allow the claims.

Conclusion

Applicants maintain that the integrated development environment for the design of software proffered by Bowman-Amuah '364 does not teach nor suggest that the relationships between three security subsystems determine the properties and functions of an information handling system, as claimed in independent claims 1 and 7 of Applicants' invention. Bowman-Amuah '364 merely provides a laundry list of security functions and components but doesn't state how they are to be integrated during the design process; Bowman-Amuah '364, moreover, states that its audit security function is independent from the development environment. Alsberg '572 teaches that security functions are best handled by a separate server between the components of an information handling system in order to avoid the precise design and redesign required for a system to handle ever-changing security threats. The combination of Bowman-Amuah '364 and Alsberg '572 with Leighton '778, moreover, does not teach the three subsystems integrated into security wherein the risks to the auditing, the risks to the integrity, and the risks to the information flow control subsystems are ranked. Merely ranking users' security as taught by Leighton '778 does not design security into an information handling system. Applicants claim a novel and nonobvious framework and method to design a secure information handling system wherein audit, information control, and integrity security subsystems and the interconnectedness between them determine the properties, functions, infrastructure, components, and operations of the system.

Attorney for Applicants thank the Examiner for her examination of the application. Applicants have thus amended the claims to place the application in condition for allowance. The Examiner is further invited to telephone the Attorney listed below if she thinks it would expedite the prosecution and the issuance of the patent.

Respectfully submitted,

Date: 09 May 2006

Karuna Ojanen
Registration No. 32,484
(507) 269-6622 voice

OLO - Ojanen Law Offices
2665 Riverside Lane, NE
Rochester, MN 55906-3456

54462
54462
PATENT TRADEMARK OFFICE